Volume 17, Issue 09   Atari Online News, Etc.   February 27, 2015

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1709   02/27/15

~ Superfish Removal Tool! ~ People Are Talking!   ~ Google Chrome Update
~ Doom: Use Selfie Stick ~ Club Nintendo Details! ~ Lenovo.com Hacked!
~ EU Police Remove Botnet ~ HAL Wins Atari Games! ~ Google Scrubs Pwnium!

         ~ ISPs Plan Challenges!   ~ Porn Loses, Then Wins! ~ Bitcoin Exchange Hack!

                    -* FCC Passes Net Neutrality! *-
                  -* Atari Pioneer Steve Bristow Passes! *-
               -* NSA Director Wants Access to Encrypted Data *-

                                =~=~=~=

->From the Editor's Keyboard   "Saying it like it is!"
   """""""""""""""""""""""""""

Believe it or not, there weer no major snow storms here this week! I know,
I find it hard to believe myself, but it's true. However, the frigid
te,peratures continue to plague most of the Northeast, so little existing
snow is melting away! Supposedly, Spring arrives in three weeks! Sure,
perhaps according to the calendar!

Lots of important news coming your way this week. A lot of this week's
issue deals with the FCC's passage of their Net Neutrality regulations.
There's a lot to digest in these articles, so you may want to check them
out and then do so again to try and understand how these new regs affect
us all. I'll leave you all to that, so let's dive right in, shall we!

Until next time...

                                =~=~=~=

->In This Week's Gaming Section - New Mod Lets You Use a Selfie Stick in Doom!

   """"""""""""""""""""""""""""""""   Atari Pioneer Steve Bristow Passes Away!
                                       HAL Wins: Bests Humans at 'Space Invaders'!
                                       And more!

                                =~=~=~=

->A-ONE's Game Console Industry News   - The Latest Gaming News!
   """""""""""""""""""""""""""""""""""""

                New Mod Lets You Use a Selfie Stick in Doom

Just when we thought the year of the selfie was coming to a close, the
selfie stick brought it all back. Now a modder is sending them to Mars.

InstaDoom is a new mod from DoomWorld user Linguica that adds a selfie mode to the 22-year-old first-person shooter.

The ability to take a selfie, as seen in Grand Theft Auto V and The Legend of Zelda: Wind Waker on Wii U, was a huge step up from simply taking a screenshot in the gaming days of yore. It turned the act of taking a picture into an action actually carried out by your character in-game. But do you think Doomguy, master of ridiculous armaments and wielder of the BFG, would be content with pedestrian arm s-length selfies?

Surely not. He carries a BFSS.

With the mod installed, certain weapon drops throughout the game have been replaced with the selfie stick. It really ups your selfie game just look at that framing!

Of course, the Mars-invading denizens of Hell respond about as well to Doomguy s selfie stick as we do to that tourist at the Met, so you might have to put down the camera and defend yourself from time to time. Luckily this leaves you with a nice pile of corpses to backdrop your next shot. Remember to observe the rule of thirds!

Once you re done taking that shot, be sure to tweak it for maximum Facebook impact by adding one of the 37 included Instagram-style hipster color filters. Hell looks great in Valencia.

Club Nintendo Program Discontinuation Details

Important Information on Club Nintendo Program Discontinuation

Dear Club Nintendo members,

Thank you for your continued loyalty to Nintendo. We launched Club Nintendo 6 years ago in North America, and we re grateful for all of the feedback that our members have provided on your experiences with our products. In order to focus on planning for a new customer loyalty program for our fans, we ve decided to wind-down the Club Nintendo program.

We are deeply thankful to our members for being a part of Club Nintendo for all of these years. We will share details about our new program at a later date. For now, please see the schedule below for information on the discontinuation timeframe for Club Nintendo.

All Coins will be deleted when Club Nintendo accounts are closed on July 1, 2015. As a result, to give our members the best opportunity to use their Coins, we have added dozens of downloadable games and a limited quantity of exclusive reward items to the rewards catalog. In addition, as a small token of appreciation for your loyalty, all Club Nintendo members are receiving a free download code for Flipnote Studio 3D.

Club Nintendo program discontinuation schedule

1/20/2015 Products released after this date are not eligible for registration with Club Nintendo
3/31/2015 Last day to earn Coins, register products with Club Nintendo,

and sign up for new Club Nintendo membership
6/30/2015 Last day to redeem Coins or access your account on the Club
Nintendo website. Club Nintendo program shuts down at 11:59pm PT on
6/30/2015.

Your Account and Coin Balance

The information in your Club Nintendo account will not be transferred to
the new loyalty program. We have added multiple items to our reward
catalog, so please be sure to redeem your Coins before the deadline on
June 30, 2015. Unused Coins will be deleted as of July 1, 2015.

2015 Elite Status

In order to reach Elite Status, you must earn 300 Coins (for Gold Status)
or 600 Coins (for Platinum Status) between July 1, 2014 and March 31,
2015. Members who reach Elite Status will be able to choose a
downloadable game from a wide selection of Nintendo 3DS and Wii U
titles. Your free Elite Status gift will be available between April 1
and April 30, 2015. A list of the Elite Status 2015 gifts will be
posted once announced.

FAQs about Club Nintendo program discontinuation

How long can I keep earning Coins?

The last day to register products with Club Nintendo, take surveys, or
earn Coins is March 31, 2015. Surveys in your To-Do list will be deleted
after March 31, 2015, so please be sure to register products or take
surveys by that date. Please note that products released after January 20,
2015 cannot be registered at Club Nintendo, and will not be eligible for
surveys or Coins.

But I have a Club Nintendo PIN # that is valid past March 31, 2015.

Products cannot be registered after March 31, 2015, regardless of the
expiration date written on the PIN card.

Will the games I download still be registered with Club Nintendo?

Club Nintendo-eligible games that you download will continue to be
registered to your account automatically until March 31, 2015 if your
Nintendo eShop account is linked to your Club Nintendo account. After
that date, games will no longer be registered with Club Nintendo. To find
out which games you can register, please see Eligible Products.

When is the last day to join Club Nintendo?

You can join Club Nintendo until March 31, 2015.

When is the last day to redeem Coins on Club Nintendo?

The last day to redeem your Coins is June 30, 2015. Any unused Coins
will be deleted on July 1, 2015. We are offering a large number of
digital games, and select physical rewards, so we are sure you can find
something you like. Limited quantities are available for the physical
rewards, so please be sure to check out our Get Games & Rewards page for
each item s availability.

What happens to my Coins if I don?t use them all?

Any unused Coins in your Club Nintendo account will be deleted on July 1, 2015.

When is the last day to get the download code for the digital games I chose?

The last day to access your Club Nintendo account is June 30, 2015, so please be sure to get your 16-digit download code(s) for any games you ve received before that date.

Will the download code ever expire?

Yes, all download codes redeemed from Club Nintendo will expire on July 31, 2015, so please be sure to download your game from the Nintendo eShop before that date.

Do I need to cancel my membership?

No, your account will automatically be cancelled on July 1, 2015, so there is no need for you to cancel your account.

                              =~=~=~=

->A-ONE Gaming Online   -   Online Users Growl & Purr!
   """""""""""""""""""""

                  Atari Pioneer Steve Bristow Passes Away

Atari engineer Steve Bristow, an early employee who conceptualized Breakout and was instrumental in designing the Atari 2600, has passed away. Company founder Nolan Bushnell has previously described Bristow as a games industry pioneer.

The Atari Museum's Marty Goldberg shared the news on Facebook. Bristow died Sunday.

Bristow got his start at Atari working on arcade games, including Indy 800 and Tank. He later held a number of executive-level positions at the company, including vice president of engineering where he helped birth the popular Atari 2600 home console.

Prior to joining Atari, Bristow worked for Bushnell at Nutting Associates as an intern on Computer Space, considered to be the world's first arcade game.

Bristow officially left Atari in 1984.

Atari has changed dramatically since its heyday in the early eighties. The company is moving forward under new management, and just recently announced an Asteroids MMO for PC.

Computers already have bested human champions in "Jeopardy!" and chess, but artificial intelligence now has gone to master an entirely new level: "Space Invaders."

Google scientists have cooked up software that can do better than humans on dozens of Atari video games from the 1980s, like video pinball, boxing, and 'Breakout.' But computers don't seem to have a ghost of a chance at "Ms. Pac-Man."

The aim is not to make video games a spectator sport, turning couch potatoes who play games into couch potatoes who watch computers play games. The real accomplishment: computers that can teach themselves to succeed at tasks, learning from scratch, trial and error, just like humans.

The computer program, called Deep Q-network, wasn't given much in the way of instructions to start, but in time it did better than humans in 29 out of 49 games and in some cases, like video pinball, it did 26 times better, according to a new study released Wednesday by the journal Nature. It's a first time an artificial intelligence program bridged different type of learning systems, said study author Demis Hassabis of Google DeepMind in London.

Deep Q "can learn and adapt to unexpected things," Hassabis said in a news conference. "These types of systems are more human-like in the way they learn."

In the submarine game "Seaquest," Deep Q came up with a strategy that the scientists had never considered.

"It's definitely fun to see computers discover things that you didn't figure out yourself," said study co-author Volodymyr Mnih, also of Google.

Sebastian Thrun, director of the Artificial Intelligence Laboratory at Stanford University, who wasn't part of the research, said in an email: "This is very impressive. Most people don't understand how far (artificial intelligence) has come. And this is just the beginning."

Nothing about Deep Q is customized to Atari or to a specific game. The idea is to create a "general learning system" that can figure tasks out by trial and error and eventually to stuff even humans have difficulty with, Hassabis said. This program, he said, "is the first rung of the ladder."

Carnegie Mellon University computer science professor Emma Brunskill, who also wasn't part of the study, said this learning despite lack of customization "brings us closer to having general purpose agents equipped to work well at learning a large range of tasks, instead of just chess or just 'Jeopardy!'"
To go from pixels on a screen to making decisions on what to do next, without even a hint of pre-programmed guidance, "is really exciting," Brunskill said. "We do that as people."

The idea is that when the system gets scaled up, maybe it could work like asking a phone to plan a complete trip to Europe, book all the flights and hotels on its own "and it sorts it all out as if you have a personal

assistant," Hassabis said.

But to some ways of thinking, Deep Q wasn't even as smart as a toddler because it can't transfer learned experiences from one situation to another and it doesn't get abstract concepts, Hassabis said.

Deep Q had trouble with "Ms. Pac Man" and "Montezuma's Revenge" because they are games that involve more planning ahead, he said.

Next, the scientists will try the system on more complicated games of the 1990s and beyond, perhaps a complicated game like "Civilization," where gamers create an entire empire to see if it can stand the test of time.

Deep Q isn't showing what Hassabis would call creativity, he said: "I would call it figuring out something that already existed in the world."

Creativity would be if the program created its own computer game, Hassabis said. Artificial intelligence isn't there, he said.

At least not yet.

                          =~=~=~=

                    A-ONE's Headline News
                The Latest in Computer Technology News
                     Compiled by: Dana P. Jacobson

            FCC Chief Pressed To Release Net Neutrality Rules

A key Republican lawmaker in Congress called for Federal Communications Commission Chairman Tom Wheeler to make proposed net neutrality regulations public before a planned Thursday vote on the measure.

In the latest wrinkle in the Republicans' battle to quash Wheeler's proposals, Rep. Jason Chaffetz, R-Utah, who's also the chairman of the House Oversight Committee, sent a letter today to Wheeler, questioning whether the FCC has been "independent, fair and transparent" in crafting the rules to protect content on the Internet.

"Although arguably one of the most sweeping new rules in the commission's history, the process was conducted without using many of the tools at the chairman's disposal to ensure transparency and public review," he said.

Chaffetz urged Wheeler to publicly release the 332-page draft order that was given to the other four commissioners nearly three weeks ago and appear at a House Oversight hearing Wednesday before a vote at the FCC's monthly meeting Thursday.

Also, FCC commissioners Ajit Pai and Michael O'Rielly too asked for Wheeler to release the proposal to the public and postpone the Thursday vote to allow for 30 days of public comment.

He also asked Wheeler to reconsider testifying at a House Committee on

Oversight & Government Reform hearing Wednesday and allow for a period of public review before the FCC votes on the regulations.

The FCC has been recasting net neutrality rules because the agency's 2010 rules were tossed out by a federal court last year. Rules for net neutrality, or open Internet, would ensure that Internet service providers (ISPs) give consumers access to all legal content and applications on an equal basis, without favoring or blocking some sources. The rules would also prohibit ISPs from allowing content providers to pay to get speedier delivery of their content, a practice known as "paid prioritization."

Sides have been drawn over how Wheeler has crafted the new rules. He based the legal authority of his proposal on parts of both the Communications Act of 1934 and the Telecommunications Act of 1996.

Consumer advocates supported the use of Title II of The Communications Act to regulate ISPs as if the Net were a utility, as is traditional telephone service. But critics say that could give the FCC too much regulatory power.

Originally, Wheeler had planned a different approach, but changed his strategy. His announcement of that shift came after President Obama in November called for tough net neutrality rules based on Title II.

Since then, two congressional committee chairmen have asked Wheeler and the FCC whether Obama exerted undue influence on the process. And draft congressional legislation proposes a measure that supporters say would be less intrusive because it doesn't rely on Title II, but would still ban ISPs from blocking or deliberately slowing content, as well as prohibiting paid prioritization for fast lanes.

Earlier this month, FCC commissioner Pai called for Wheeler to make the net neutrality proposal public. "With the future of the entire Internet at stake, it is imperative that the FCC get this right," he and O'Rielly said in their statement today. "And to do that, we must live up to the highest standards of transparency."

In his response to an earlier congressional request to make the proposals public, Wheeler said the FCC had received more than 4 million comments and held six public roundtables. Releasing the rules before the commission votes runs contrary to how federal agencies work, he said. "If decades of precedent are to be changed, then there must be an opportunity for thoughtful review in the lead up to any change," Wheeler wrote.

Kim Hart, press secretary to the FCC chairman, said that "the chairman has seriously considered all input he has received on this important matter, including feedback from his FCC colleagues."

There is precedence for the FCC chairman to make rules public, the commissioners and Rep. Chaffetz said. In 2007, then-chairman Kevin Martin released to the public new media ownership rules and the entire FCC testified in a House hearing prior to the final vote in December.

A senator who supported the FCC's postponement back then, Chaffetz notes, was then-senator Barack Obama. "He specifically noted while a certain proposal 'may pass the muster of a federal court, Congress and the public have the right to review any specific proposal and decide whether or not it constitutes sound policy. And the commission has the responsibility

to defend any new proposal in public discourse and debate,'" Chaffetz
said citing the original letter sent by Sen. Obama to Martin.

 Locked and Loaded : FCC Primed for Vote on Internet Regs, Amid 11th-hour Drama

The Federal Communications Commission is driving toward a landmark vote
Thursday on a sweeping plan that critics warn would impose a new era of
regulation for how Americans use and do business on the Internet, even as
11th-hour appeals inject added drama behind the scenes.

The so-called net neutrality proposal has been the subject of fierce
debate, in part because the 332-page plan is being kept from public eyes.
President Obama's vocal push for aggressive Internet rules also has
raised questions on Capitol Hill over undue influence by the White House
- but House Republicans who had planned a hearing on that very subject
said Wednesday they would postpone after Chairman Tom Wheeler allegedly
refused to testify.

"This fight continues as the future of the Internet is at stake," House
oversight committee Chairman Jason Chaffetz, R-Utah, and House Energy and
Commerce Committee Chairman Fred Upton, R-Mich., vowed, in a statement
announcing the hearing delay.

For now, the plan is in the FCC's hands.

At issue is a proposal that proponents say would ensure an "open"
Internet, by growing the government's power to oversee Internet service
providers and establish new rules to bar companies from blocking or
slowing data.

But The Hill reports that a vital Democratic member, Mignon Clyburn, is
now seeking last-minute changes to scale back Wheeler's proposal.

This puts Wheeler in a tough spot because the FCC is composed of three
Democrats and two Republicans. The Republicans are likely to oppose the
plan, and Wheeler would need Clyburn on board to push it through.

According to The Hill, Clyburn would leave alone the most controversial
plank of the proposal - a call to regulate broadband Internet as a
telecommunications service, treating it much like telephones.

But she reportedly wants to strip a new legal category that would give
the FCC additional legal authority over certain deals over back-end
Internet traffic.

Her requests may be in the weeds, but they have the effect of potentially
complicating Thursday's vote. The two Republican members, Ajit Pai and
Mike O'Rielly, earlier this week already urged Wheeler to postpone that
vote - and to release the plan so the public can review it. Wheeler so
far has not agreed to do so. Wheeler needs a three-member majority to
approve the plan.

Asked about the report in The Hill, Clyburn's office said she would not
comment "on any potential changes to the Open Internet Order out of
respect for the deliberative process."

Her office said: "Any reports about policy or position shifts when it comes to the item have not been verified or confirmed by her office. Commissioner Clyburn continues to advocate for strong open Internet protections for consumers and looks forward to voting the item on Thursday."

Still, Clyburn's supposed requests may not be a deal-breaker.

One FCC official told FoxNews.com there appears to be little sign of the vote being delayed.

"They are very locked and loaded with this whole thing," the official said.

Pai and O'Rielly, meanwhile, have made their position clear. Pai tweeted a photo of himself with the proposal on Wednesday, announcing that he would oppose it.

While Wheeler and consumer groups say the proposal is necessary to prevent providers from creating slow or fast Internet lanes in which content companies like Netflix can pay to jump to the head of the queue, Pai co-authored a Politico op-ed with Federal Election Commission member Lee Goodman describing the plan as "heavy-handed."

They said it would allow the FCC to regulate broadband rates; "decree" whether companies can offer "consumer-friendly service plans" like unlimited access to streaming music; and claim the power to force companies to "physically deploy broadband infrastructure."

The commissioners argued that the panel was conjuring the idea of "digital dysfunction" in order to "justify a public-sector power grab."

Wheeler, though, has pushed back on the calls for a delay.

He tweeted earlier this week that the future of the "open Internet" is at stake, and, "We cannot afford to delay finally adopting enforceable rules to protect consumers & innovators." He also noted that the commission received "more than 4 million comments on #OpenInternet during past year that helped shape proposal."
"It's time to act," Wheeler tweeted.

Asked Tuesday about the call for a delay, an FCC spokesperson also told FoxNews.com that the 4 million comments amounted to an "unprecedented" level of public response.

"In accordance with long-standing FCC process followed in both Democratic and Republican administrations, Chairman Wheeler circulated his proposal to his fellow Commissioners for review three weeks before the scheduled vote. The Chairman has seriously considered all input he has received on this important matter, including feedback from his FCC colleagues," the spokesperson said.

Even if the FCC approves the plan on Thursday, the next stop may be the courts. Industry lobbyists say it's likely that one of the major providers will sue and ask the court to suspend enforcement pending appeal.

Meanwhile, The New York Times reports that efforts by Hill Republicans to fight the plan with legislation appear to be fading.

''We're not going to get a signed bill that doesn't have Democrats' support," Sen. John Thune, R-S.D., told the newspaper, though his office later pushed back on the notion that Republicans were giving up on the issue.

FCC To Vote To Regulate Net Neutrality Thursday: What It Means

The Federal Communications Commission is set to vote Thursday on a new set of rules for Internet service providers. And while Democratic Chairman Tom Wheeler s proposal to regulate the Internet like water, electricity and other public utilities is slated for approval, the months (years, actually) of fighting over net neutrality, both within the FCC and on Capitol Hill, won t likely end there. As Thursday s vote has drawn closer, Wheeler continued to face pressure from within his own party to amend the net neutrality rules. And contrary to a report in The New York Times on Tuesday suggesting that Republican lawmakers once poised to pounce on new FCC rules with counteracting legislation have now accepted defeat, Republican Senator and Senate Commerce Committee Chairman John Thune tweeted that the GOP has far from conceded on the hot topic.

Beyond the response on Capitol Hill, the FCC can almost certainly expect a legal challenge to the new rules from the Internet service providers it seeks to regulate. So for all those who ve avoided the net neutrality conversation, it s not too late. In fact, there s no better time to start paying attention. Sure, net neutrality isn t exactly riveting date or dinner party fodder. But while friends and neighbors might not be impressed with your ability to rattle off the arguments for and against federally regulated Internet service, the direct impact that Thursday's vote and its inevitable fallout could have on your life and, more important, your wallet make it worth familiarizing yourself with the issue. But fear not. Net neutrality, and the heated debate that s surrounded it, aren t nearly as bewildering as they seem. Seriously.

What is net neutrality?

Before even attempting to tackle the politics of Thursday s vote, we need to get one thing straight: What is net neutrality? The elusive term, coined by Columbia Law School Professor Tim Wu in 2003, refers to the concept of an open Internet, wherein all data from music-sharing sites to social networks to personal blogs exists on a level playing field, free from discrimination.

Discrimination, in this sense, means the ability of Internet service providers (or ISPs), like Comcast, Verizon or AT&T, to act as Internet gatekeepers; Controlling not only which websites, apps, or other content are available online, but the speed at which that content may be accessed. In other words, if an ISP like Comcast charged a premium for faster service, it would give the Internet s big money-makers a major leg up over smaller, less profitable sites. Not only would users be forced to choose between waiting a painfully long time to download a song for free on Soundcloud and paying to listen instantly on iTunes, ISP fees might push sites like YouTube to start charging for things we ve long grown accustomed to receiving for free.

Beyond that, there is the chance that service providers would give preferential treatment to the companies with which they collaborate. For

example, Verizon could make it so that the websites of smartphone companies that use Verizon s mobile service work faster than the websites of other smartphone companies.

Ultimately, the Internet has the potential to become exclusive, limited, and very costly which, net neutrality advocates argue, would violate what many see as a human right to Internet access.

How did this become a political debate?

Without going too far back in history, the current debate can be traced back to a federal appeals court ruling from January 2014. Siding with Verizon in a suit against the FCC, the U.S. Court of Appeals for the District of Columbia struck down a set of net neutrality rules the FCC adopted in 2010. More than a decade earlier, before the Internet evolved into its current form, the FCC had specificly chosen not to classify broadband Internet as a classic telecommunications service. Therefore, the court ruled, broadband providers were not subject to the same "common carrier" rules that telephone companies, for example, must adhere to.

In response to this ruling, last November President Obama called on the FCC to enforce net neutrality with the strongest possible rules, urging the commission to reclassify Internet service providers under Title II of the 1934 Communications Act in order to regulate the Internet like a public utility. Obama s call to action was met with challenges from Republican lawmakers like Senator Ted Cruz, who charged that net neutrality actually threatens the freedom of the Internet and would hinder the growth of the tech industry. Net neutrality is Obamacare for the Internet, Cruz wrote in a Washington Post op-ed. It would put the government in charge of determining Internet pricing, terms of service and what types of products and services can be delivered, leading to fewer choices, fewer opportunities and higher prices. On the contrary, Democratic Senator Al Franken argued on CNN in response to Cruz s claims, Obamacare was a government program that fixed something, that changed things. This is about reclassifying something so it stays the same. This would keep things exactly the same as they ve been. Yet FCC Chairman Tom Wheeler s announcement earlier this month that he planned to propose the strongest open Internet protections ever proposed by the FCC, was seen by Republicans as direct evidence of the President s influence over the commission. It s a power grab for the federal government by the chairman of a supposedly independent agency who finally succumbed to the bully tactics of political activists and the president himself, Thune said of Wheeler s announcement, arguing that what might have worked to combat telecommunication monopolies in the 1930s has no place in today s high-tech economy.

 Regulating the Internet through ill-suited and antiquated authorities that were designed for the monopoly phone era will ultimately make the Internet more rigid and less innovative, Thune said.

Senate Republicans ultimately tabled an earlier plan to put out legislation ahead of the FCC vote. But Thune s recent tweet suggests he still has every intention to try to override Wheeler s rules in Congress. And while the FCC has received overwhelming support from Internet companies from Google to Netflix to Etsy, Internet service provider giants like AT&T have already promised to sue the FCC if Wheeler s rules are approved.

The FCC's last attempt to impose rules on ISPs may have ended in a

lawsuit, but Wheeler told the tech site CNET in an interview last month that he's confident his new rules can stand up to the challenge.

"We think we have a clear legal case," Wheeler said. "I can assure you that we are writing this with the full expectation that it will be reviewed by the court, so we will make sure we are on sound footing."

U.S. Internet Providers Hit With Tougher Rules, Plan Challenges

U.S. regulators on Thursday approved the strictest-ever rules on Internet providers, who in turn pledged to battle the new restrictions in the courts and Congress, saying they would discourage investment and stifle innovation.

The rules, which will go into effect in coming weeks, are expected to face legal challenges from multiple parties such as wireless, cable and other broadband companies and trade groups that represent them.

Experts expect the industry to seek a stay of the rules, first at the FCC and then in courts, though the chances for success of such an appeal is unclear.

The new regulations come after a year of jostling between cable and telecom companies and net neutrality advocates, which included web startups. It culminated in the FCC receiving a record 4 million comments and a call from President Barack Obama to adopt the strongest rules possible.

The agency's new policy, approved as expected along party lines, reclassifies broadband, both fixed and mobile, as a more heavily regulated "telecommunications service," more like a traditional telephone service.

In the past, broadband was classified as a more lightly regulated "information service," which factored into a federal court's rejection of the FCC's previous set of rules in January 2014.

The shift gives the FCC more authority to police various types of deals between providers such as Comcast Corp and content companies such as Netflix Inc to ensure they are just and reasonable for consumers and competitors.

Internet providers will be banned from blocking or slowing any traffic and from striking deals with content companies, known as paid prioritization, for smoother delivery of traffic to consumers.

The FCC also expands its oversight power to so-called interconnection deals, in which content companies pay broadband providers to connect with their networks. The FCC would review complaints on a case-by-case basis.

Republican FCC commissioners, who see the new rules as a government power grab, delivered lengthy dissents. Their colleagues in Congress hope to counter the new rules with legislation. All five FCC members are expected to testify in the Senate on March 18.

Large Internet providers say they support the no-blocking and no-discrimination principles of the new rules but that the FCC's

regulatory path will discourage investment by lowering returns and limiting experimentation with services and business plans.

Some smaller telecoms, such as Sprint Corp and T-Mobile US Inc , have argued new rules will have little impact on investments. FCC Chairman Tom Wheeler on Thursday agreed.

"The (Internet service providers') revenue stream will be the same tomorrow as it was yesterday," he said at the FCC meeting.

"I have spent a lot of time in public policy, and today is the proudest day of my public policy life," he later told reporters.

Legal experts and industry lobbyists say corporate lawyers are waiting for the FCC to publish the specifics of the rules, a document more than 300 pages long. Lawsuits can be filed after the rules are recorded in the Federal Register, likely days later.

Wheeler sought to address in the new rules some Internet providers' concerns, proposing no price regulations, tariffs or requirements to give competitors access to networks.

Cable and telecom shares saw muted reactions on Thursday. They had jumped earlier this month when Wheeler confirmed long-bubbling expectations that he would seek a tougher regulatory regime, with some adjustments to the network needs.

FCC Passes Net Neutrality: What This Means for Americans

After almost a year of fierce national debate, the Federal Communications Commission voted Thursday to pass net neutrality in a 3-to-2 partisan vote. The five-member commission reclassified broadband Internet access as a common carrier under Title II of the Telecommunications Act, making the Internet a regulated utility like water or electricity.

The new rules aim to ensure that Internet service providers (ISPs) cannot discriminate between content-makers by blocking or deliberately slowing some content while offering prioritization for those willing or able to pay. Mobile data service for smartphones and tablets also are being placed under the new rules. The directive also includes requirements to protect consumer privacy and to ensure Internet service is available for people with disabilities and in remote areas.

Critics of the rules say they may hinder innovation and investment. Opponents have said they plan to challenge the FCC order in court. But Republicans on Capitol Hill announced Tuesday that they do not plan to pass a legislative response.

Net neutrality, or an open Internet, is the concept that ISPs should give consumers equal access to all legal content and applications. That means ISPs could not favor or block some content-makers or charge them to provide faster delivery of their content, in what are known as fast lanes. ISPs would also be forbidden from slowing the content of competing providers.

Supporters of net neutrality say the Internet has become a human right that should be equally accessible for everyone. Denying access or giving

preferential treatment to one user over another is thus considered a violation of the user s rights.

"The Internet, which was once a luxury, is now a necessity, and it has given people the ability to be heard in our democracy and have more opportunity in our economy," Rashad Robinson, executive director of ColorOfChange, an online civil rights organization, was quoted as saying in USA Today. "It has been a tool for the little guy to get ahead."

Proponents of net neutrality say that without the new rules, smaller content providers unable to pay hefty fees to ISPs would be pushed out and made more difficult to access.

 No one should have to ask permission to innovate, and we need to retain the ability of all Internet users to communicate and compete on a level playing field, preventing the presence of fast and slow lanes that are contrary to the essence of the Internet, Sen. Edward J. Markey (D) of Massachusetts said in a statement.

Many larger Internet companies such as Netflix and Amazon, both of whose streaming services use large amounts of bandwidth, support the idea of net neutrality. Google and Twitter also are supporters.

"More than 30 percent of Internet traffic at peak times comes from Netflix, according to studies. So Verizon might say, 'Netflix, you need to pay us more,' " NPR s Laura Sydell explains. "Or maybe Verizon strikes a deal with Amazon and says your prime video service can get speedier delivery to the home and we're going to slow down Netflix.

If companies are asked to pay more, consumers may be asked to foot the bill, observers say.

But those who oppose net neutrality say it is an issue of free enterprise: Service providers should be free to decide how they deliver content and charge customers for their services. They also claim that net neutrality will prevent ISPs from making network upgrades and finding new business models.

 The last thing we should want is President Obama or a government agency picking winners and losers on the Internet. And enforcing net neutrality is picking winners and losers even if it looks like it is just leveling the playing field.' He may think it is not, but it completely blocks certain business models and stops any possible innovation that might emerge if given the option of seeking differential access to bandwidth, writes Jeffrey Dorfman in Forbes.

  'Net Neutrality' is Obamacare for the Internet; the Internet should not operate at the speed of the government, wrote Republican Sen. Ted Cruz in a tweet last November.

Furthermore, more than just the Internet is at stake, some say.

 Advocates for pay-TV providers are saying the FCC should use Section 706 to act more aggressively against the companies that produce TV content. Why? Because the pay-TV providers think the content producers are charging them too much for programming and because programming costs eat into the budget for building, say, cable broadband, writes Brian Fung in The Washington Post.

If the FCC decides to pursue this line of logic, it could affect how much

consumers pay for cable providers, too.

What every side does agree on, though, is that the results of today s vote
will affect everyone who uses the Internet. Anyone who goes online does so
through an ISP, and increasingly these companies are lobbying to provide
services on their own terms. Without net neutrality rules, companies like
Comcast and Verizon could cherry pick which content is easy to access. And
that means that consumer access to specific online content could slow down
or speed up noticeably.

For anyone who uses the Internet, around 87 percent of Americans, today's
vote is a really big deal.

NSA Director Wants Gov't Access To Encrypted Communications

It probably comes as no surprise that the director of the U.S. National
Security Agency wants access to encrypted data on computers and other
devices.

The U.S. should be able to craft a policy that allows the NSA and law
enforcement agencies to read encrypted data when they need to, NSA
director Michael Rogers said during an appearance at a cybersecurity
policy event Monday.

Asked if the U.S. government should have backdoors to encrypted devices,
Rogers said the U.S. government needs to develop a framework.

 You don t want the FBI and you don t want the NSA unilaterally deciding,
 So, what are we going to access and what are we not going to access?
Rogers said during his appearance at the New America Foundation. That
shouldn t be for us. I just believe that this is achievable. We ll have
to work our way through it.

Justsecurity.org has a transcript of an exchange between Rogers and Yahoo
CISO Alex Stamos at Monday s event.

Rogers isn t the first member of President Barack Obama s administration
to call for encryption workarounds in recent months. In September, after
Apple and Google announced encryption features on their smartphone OSes,
both FBI Director James Comey and Attorney General Eric Holder raised
concerns that additional encryption tools would hinder law enforcement
investigations.

Stamos questioned whether it is a good idea to build backdoors in
encryption. If we re going to build defects/backdoors or golden master
keys for the U.S. government, do you believe we should do so .... for the
Chinese government, the Russian government, the Saudi Arabian government,
the Israeli government, the French government? he said, according to the
Justsecurity transcript.

Rogers objected to using the word backdoor . When I hear the phrase
 backdoor , I think, Well, this is kind of shady. Why would you want to
go in the backdoor? It would be very public, he said. Again, my view
is: We can create a legal framework for how we do this. It isn t
something we have to hide, per se.

An NSA spokeswoman wasn t immediately available for further comment.

EU Police Operation Takes Down Malicious Computer Network

European police have taken down a computer network that used malicious software to infect more than 3 million computers worldwide and steal personal data, banking details and passwords.

European Union police coordination agency Europol said in a statement Wednesday that the network, known as the Ramnit botnet, was dismantled in an operation Tuesday by cybercrime experts coordinated from Europol s headquarters in The Hague.

The operation involving investigators from Germany, Italy, the Netherlands and Britain along with representatives from companies including Microsoft and Symantec shut down control servers and redirected Internet domain addresses used by the network s criminal operators.

Symantec says in a statement that the network had been operating for at least five years and evolved into a major criminal enterprise that defrauded large numbers of victims.

Lenovo Releases Superfish Removal Tool

Chinese PC maker Lenovo late yesterday (Feb. 20) released a removal tool for the dangerous Superfish adware that Lenovo had pre-installed on many of its consumer laptops. Hours later, a security researcher demonstrated how easily the adware could be used to hack into online financial transactions.

The Lenovo Superfish removal tool can be found at http://support.lenovo.com/us/en/product_security/superfish_uninstall. It must be downloaded first, but will run without installation. Lenovo has released the tool under a public license and placed the source code on the developer website Github so that security experts can analyze and possibly improve on it.

(If you have a Lenovo laptop, you can check whether it is affected by using each installed Web browser to visit https://filippo.io/Badfish/.)

Early today (Feb. 21), Robert Graham, CEO of Atlanta-based Errata Security, posted detailed instructions on his blog on how to create a malicious Wi-Fi hotspot to exploit the security vulnerability that the Superfish adware creates on Lenovo laptops.

"This example proves that this exploit is practical, not merely theoretical, as claimed by the Lenovo CTO," Graham wrote.

Graham used a Raspberry Pi 2, which is a minicomputer that costs about $35, a $10 Wi-Fi adapter and a microSD card, which can be had for as little as $4. The software was all freely downloaded from the Internet, and it took Graham about 3 hours to build the device and get it running.

To demonstrate the flaw, he used a laptop on which the Superfish adware had been installed to connect to the Internet using his malicious

hotspot. He tried to log into the Bank of America website using a fictitious name, and showed that the hotspot intercepted the connection and logged the fictitious name. It would also have logged the password, had there been one.

For about $50, a malicious hacker could build a similar hotspot, name it "Starbucks HotSpot" and bring it into your local coffeeshop. Any user of an affected Lenovo laptop who connected to the Internet using that hotspot could have all her or his banking, social-media and shopping sessions intercepted and decrypted.

Superfish is an American-Israeli company, and its adware, called Visual Discovery, analyzes images of retail products displayed in a Web page, then adds advertisements showing similar or identical products for sale at other locations online. This is done without the consent of the website operator or the laptop user.

Many forms of unwanted adware can pull off this trick on unencrypted Web pages, but Superfish goes further. By breaking the Web browser's system of secure connections, it can inject ads even into encrypted "HTTPS" websites, such a secure retail site -- or a banking website.

Superfish can do this because Lenovo pre-installed the adware and added Superfish's digital signature to the list of "root certificates" that Windows trusts to guarantee a secure Web connection. As a secure Web page's information travels from the network connection (either an Ethernet port or Wi-Fi card) to the Web browser, Superfish intercepts it, decrypts it, adds its own ads, then re-encrypts it using its root certificate.

The laptop user will be none the wiser, and will believe he or she is still viewing a secure Website. Because this "man-in-the-middle attack" takes place entirely within the computer, the website operator will not be aware that the secure connection has been broken.

That's arguably unethical, but wouldn't be inherently dangerous it had every Lenovo laptop used an entirely different certificate to re-encrypt the connection.

But they don't. Every Lenovo installation of Superfish uses the same private key to verify the connection. On Thursday, Graham decrypted that universal private key and revealed that its password was "komodia."

Komodia is the name of an Israeli company that makes two pieces of software, called SSL Digestor and Redirector, made by an Israeli company called Komodia.

Security researcher Marc Rogers analyzed other pieces of software made by Komodia, including a parental-control product called "Keep My Family Secure," and said that the private keys always used the password "komodia."

Lenovo's first response when the Superfish flaw went public Thursday (Jan. 19) was to deny that there was anything to worry about.

"We have thoroughly investigated this technology and do not find any evidence to substantiate security concerns," the company said in its initial statement.

But by the end of the day, the company had changed its tune."We're

sorry. We messed up," the Lenovo U.S. Twitter feed said. "We're making sure it never happens again."

The company reiterated that the Superfish adware had been installed only on consumer laptops manufactured between September 2014 and January 2015, and would no longer be used.

However, the Superfish company was adamant in a statement to Ars Technica's Dan Goodin.

"Despite the false and misleading statements made by some media commentators and bloggers, the Superfish software does not present a security risk," a company representative told Goodin.

The Superfish company has not made any other public statement about the Lenovo situation.

Lenovo.com Has Been Hacked, Possibly by Lizard Squad

Lenovo.com has been hacked. As of 4PM ET, users visiting the site saw a slideshow of disaffected youths, set to the song Breaking Free from High School Musical. By 4:17, the site seemed to have reverted to its normal self, although HTML problems persist and in some instances, the song continued to play in the background. The hacked version has reappeared intermittently as cached versions work through the system.

The source code for the hacked page identified it as, the new and improved rebranded Lenovo website featuring Ryan King and Rory Andrew Godfrey, both of whom have been publicly identified as members of the hacker collective Lizard Squad. It s unclear whether King and Godfrey are actually related to the hack, or if the attackers are simply using their names and photos to muddle their true identity.

The hack comes on the heels of a wave of public criticism of Lenovo, after the company bundled computers with an encryption-breaking adware program known as Superfish. Lenovo eventually released a program to remove the software and restore affected users, but the debacle left many users unhappy with the company. That lingering mistrust may have contributed to the attack.

The attackers seem to have hijacked Lenovo s domain record, an attack that would have given them the power to redirect the lenovo.com url to a new server under their control. The attack targets entirely external infrastructure, similar to the Syrian Electronic Army s attacks against Twitter and The New York Times in 2013. As a result, there s no reason to believe the attackers have breached Lenovo s internal network. Still, it s an embarrassing incident for the company, particularly on the heels of security concerns over Superfish.

Google Chrome Update Curbs Harmful Software Downloads

Many of us find anti-viruses cumbersome and taxing on the computer, but remove those and the computer is susceptible to attacks from malware, spyware, phishing, fake advertising, and malicious software that can harm

or warp a computer s security measures. With social media on the rise, online privacy and protection has become one of the most integral subjects, and Google has moved to address that.

Google Chrome s next update will elaborate on the Safe Browsing feature it introduced in September 2011 to warn users before they end up visiting any potentially dangerous websites. A warning screen will pop up that will include a details section that will further clarify what makes the page in question a risky prospect for the user. All this was revealed in Lucas Ballard s blogpost, who is a software engineer at Google Inc. Any page that encourages download of an unwanted software will be flagged by Google, and will redirect users to a warning page.

The Safe Browsing techniques apply to other aspects of Google as well. Google Search will earmark these websites, and prevent them from showing up in users search results. This will at least ensure that Chrome users will not be directed to websites that will encourage them to download unwanted software. Similarly, advertisements that trick users into downloading malware will also be disabled. This will help Google raise the credibility of online ads, which are more often seen as spam rather than something users can really benefit from.

Google has been scanning for malicious content since 2008, and has a vast database that its API incorporates. As a result, Safari by Apple Inc. and Mozilla Firefox also include parts of Google s API to reinforce their searches. What makes Google s searches stronger is that the Mountain View company relies on rankings and reputation of websites to determine which ones are the most likely to include harmful content. Google, like Microsoft Corporation does with its Internet Explorer, uses a series of whitelists, blacklists, and algorithms to rank websites, and determine the probability of them carrying harmful software that will force itself onto users computers.

Of course, this might have been ineffective if a legitimate website had just started operations was flagged, having had no prior reputation. Google has a fix for that too. Site owners are encouraged to register with Google Webmaster Tools, which will inform owners when their website contains harmful content and even guide them on how to resolve such issues. This certainly falls in line with Google s promise to keep people safe across the web.

Google s apparently altruistic approach is certainly useful for Internet users at large, with the search engine siphoning through large amounts of data to fish out harmful websites from the normal ones. It will only serve to enhance the company s reputation, while reinforcing the thought that Google is everywhere. The only apparent danger is that of startup sites finding it harder to gain credibility on the Internet, and there may be a debate about net neutrality in here somewhere. For now, we can expect less spamming and more relevant results from the Mountain View-based company.

Google Scrubs Pwnium Hack Contest

Google yesterday said it would shut down its Pwnium hacking contest, which it has held alongside the better-known Pwn2Own challenge each spring since 2012.

Instead, Google will focus on its long-standing bug bounty program.

"Pwnium will change its scope significantly, from a single-day competition held once a year at a security conference to a year round, worldwide opportunity for security researchers," wrote Chrome security engineer Tim Willis in a Tuesday blog post.

Last year, Google paid out $190,000 from its Pwnium pool to two researchers who demonstrated multi-vulnerability chains that exploited Chrome OS, the search giant's browser-based operating system. George Hotz, a noted iPhone and Sony PlayStation hacker, was handed $150,000 by Google for what the firm called "an epic Pwnium competition win," while another researcher, known only as "Pinkie Pie," was awarded $40,000 for a partial exploit.

Pwnium had attracted attention for its large awards - up to $150,000 for each hack - the $3.14 million Google had pledged in 2013 to spend if necessary, and the focus on Chrome OS.

Willis took a shot or two at Pwn2Own, the hacking contest run by HP TippingPoint's Zero Day Initiative (ZDI), a rival bug bounty program, as he explained Google's reasons for folding up the Pwnium tent.

"At Pwnium competitions, a security researcher would need to have a bug chain in March, pre-register, have a physical presence at the competition location and hopefully get a good time slot," said Willis. "[And] if a security researcher was to discover a Pwnium-quality bug chain today, it's highly likely that they would wait until the contest to report it to get a cash reward. This is a bad scenario for all parties."

ZDI's Pwn2Own requires that researchers - or a representative - be physically at the contest, which is held at the CanSecWest security conference in Vancouver, British Columbia. Pwn2Own hands out cash prizes only for until-then-unknown vulnerabilities.

Rather than sponsor Pwnium, Google will boost the maximum award in its own bounty program to $50,000 for "Pwnium-style bug chains on Chrome OS," Willis added. Those rewards will be available year-round.

At times, there has been tension between Google and ZDI over hacking challenges.

In 2012, Google first said it would partner with ZDI to pitch in prize money for Pwn2Own, then withdrew that offer. Google objected to Pwn2Own rules that did not require contestants to reveal to vendors a complete exploit or all the vulnerabilities used in a demonstration.

ZDI contested Google's assertions, arguing that prize money - even the then-top $60,000 - wasn't enough to shake loose the very rare sandbox-escape vulnerabilities and ensuing exploits against the Chrome browser target.

Rather than back out completely, Google launched Pwnium, which also ran during CanSecWest.

Google will remain a sponsor of this year's Pwn2Own; its Project Zero team will not only help pay for the contest's prizes, but separately will award up to $10,000 for entries that successfully exploit the latest release of Chrome 42.

HP TippingPoint declined to comment on Google's decision to scrap Pwnium.

Pwn2Own will take place March 18-19, with $465,000 in awards up for grabs.

Accused 'Revenge Porn Site' Operator: Take Down My Private Photos

This, indeed, was the name of an alleged "revenge porn site" he once ran. Should you be unfamiliar with this thoroughly modern idea, revenge porn sites encourage the hurt or merely the hateful to post naked personal images sent to them (presumably as a gesture of love) by former paramours.

Now it seems that Brittain himself is down. He's low because personal images of, well, him are readily available via Google searches and he wants them removed.

Indeed, he's issued a takedown notice under the Digital Millennium Copyright Act, relating to "unauthorized use of photos of me and other related information. Unauthorized use of statements and identity related information. Unauthorized copying of excerpts from isanybodydown.com. Using photos which are not 'fair use.'"

On reading this, there might be one or two people invoking pots, kettles and an especially terrifying dark humor.

Indeed, one of the links that Brittain objects to is this one, which happens to be from the Federal Trade Commission.

It announces that Brittain has been banned for allegedly posting nude images without due fairness. Indeed, the FTC mused that Brittain" used deception to acquire and post intimate images of women, then referred them to another website he controlled, where they were told they could have the pictures removed if they paid hundreds of dollars."

On receiving this order, Brittain posted to his own site a 49-paragraph apologia, among whose words were: "I made a series of poor decisions, then tried to rationalize them, and made it even worse. I am sorry for the damage that I caused to everyone that ended up on my website. I am making amends at every opportunity. I regularly volunteer for, and donate to charitable organizations (I encourage you to do the same!)."

So the man who claims to have turned over a new leaf is asking Google to remove any digital leaves that bear his imprint.

However, he also added in his apologia: "I strongly believe that any law against 'revenge porn' is unconstitutional, circa Arizona, and should be overturned. This does not mean I morally support 'revenge porn,' I do not. It simply means that I don't support spending millions (billions?) in taxpayer dollars to enforce a moral issue."

Perhaps he feels that having his own images and information taken down is also a moral issue.

Google Bans Sexually Explicit Content on Blogger

Google is strapping a chastity belt onto its Blogger blogging platform.

It says that starting 23 March 2015, Blogger bloggers won't be able to publicly share images and video that are sexually explicit or show graphic nudity.

Note that any smut that's on a blog before that date won't be deleted.

Rather, it will be made private after 23 March, only viewable by the blog owner or admins and the people with whom the owner has shared the blog.

Global News reports that Google sent emails to Blogger users informing them of the policy change.

Leading up to that date, bloggers who muse about the carnal have a few choices: you can remove the sexually explicit or graphic nudies, or you can take it upon yourself to mark the blog as private.

Then again, if you'd rather pack it up and move to another, less restricted blogging platform altogether, Google suggests that you have the option of exporting your blog as an .xml file or archiving its text and images with Google Takeout.

As far as adult content-friendly platforms go, WordPress allows blogs with adult content as long as they're marked as Mature in our system .

It's not a free-for-all, however: WordPress warns against posting sexual materials that can be considered pornographic, such as images or video of explicit sexual acts or close-up images of genitalia.

Tumblr, on the other hand, tolerates sex and nudity, though such material is filtered and users have to unlock "Safe Mode" to see anything racy (which, as of this month, now includes torrent-related searches).

From Tumblr's current adult content policy:

We have no problem with that kind of stuff. Go nuts. Show nuts. Whatever.

Any salacious blogs created after 23 March will be bumped off Blogger or subjected to unspecified "other action", Google says.

That goes for blogs that include content that's "sexually explicit" or that shows graphic nudity as explained in Google's content policy.

Exempt from the purge is content that offers "a substantial public benefit", Google says, such as that found in artistic, educational, documentary, or scientific contexts.

Google didn't give any reasons for the new policy, which replaces a previous policy on Blogger that allowed adult content if it were in fact labeled as "adult".

Google hasn't changed its policy's messaging around censorship, stating that "censoring this content is contrary to a service that bases itself on freedom of expression."

How Google will manage, with Blogger, to increase "the availability of information, [encourage] healthy debate, and [make] possible new connections between people" while still curbing "abuses that threaten our ability to provide this service and the freedom of expression it

encourages" remains to be seen.

Writing policies and laws that restrict truly harmful content while still respecting freedom of speech isn't easy.

That was made apparent recently when civil liberties advocates, bookstores and publishers sued to stop an anti-revenge porn law in the US, outlining how laws that aren't written carefully enough could arguably be used to criminalize a host of non-vengeful innocents who handle nude images: libraries, booksellers, college professors or breastfeeding educators, for example.

Good luck to Google on that one.

Porn Lovers Win: Blogger Ban on Adult Content Reversed

Not even Google can erase porn from the Internet.

Just three days after banning explicit sexual content on Blogger, Google has given in to pressure from porn fans who were less than thrilled about the new policy. The Web giant on Friday announced that it has changed its mind and will not crack down on adult content on its blogging platform, after all.

The turnaround comes after Google on Tuesday said it would no longer allow "images and video that are sexually explicit or show graphic nudity" on Blogger, as of March 23. Any existing blogs containing porn would be made private, unless the admin deleted the offending content.

Now, Google says that porn will be allowed on Blogger, but asked people to tag pages with nudity, so that Blogger can display an "adult content" warning page before that content is served up.

"This week, we announced a change to Blogger's porn policy," Google's Social Product Support Manager, Jessica Pelegio, wrote in a post on the Blogger Help Forum. "We've had a ton of feedback, in particular about the introduction of a retroactive change (some people have had accounts for 10+ years), but also about the negative impact on individuals who post sexually explicit content to express their identities. So rather than implement this change, we've decided to step up enforcement around our existing policy prohibiting commercial porn."

That commercial porn ban, instated in 2013, strictly prohibits adult ads on Blogger and the monetization of adult content, meaning you can't start a blog on the site to make money off porn.

So, in other words, long live porn on the Internet.

Hackers Force Closure of Canadian Bitcoin Exchange Cavirtex

Canadian Bitcoin exchange Cavirtex has announced its imminent closure following an apparent security breach.

The exchange, believed to be Canada's biggest, has already ceased taking

new deposits and will halt withdrawals from 25 March.

The decision to close the exchange came on Sunday after it discovered that an older version of its database may have been compromised:

On February 15, 2015 we found reason to believe that an older version of our database, including 2FA secrets and hashed passwords, may have been compromised.

Fortunately, Cavirtex said that the database in question did not include identification documents.

In a statement published on Tuesday, the company elaborated on its decision to cease trading, citing uncertainty over security and potential reputational damage:

Because security and the safety of customer funds are paramount to our mission and the success of Bitcoin in general, CAVIRTEX has determined to cease active operations in the Bitcoin business and to return all customer funds. We believe that the damage to the company's reputation caused by the potential compromise will significantly harm our ability to continue to operate successfully.

As a result of the potential compromise of our database we cannot be certain of the confidentiality of account credentials.

The Cavirtex team said customer funds were not affected and the company remains solvent and fully able to cover all withdrawals made prior to its 25 March deadline.

The company urged users to change their passwords immediately and delete any Cavirtex cookies from their browsers.

Speaking to CoinDesk, Cavirtex vice president Kyle Kemper said the exchange had been targeted by hackers before, and that the protection of customer balances was becoming ever more challenging:

[The closure] has entirely to do with the fact that some of our databases were compromised. And, given the history of hackers against us, you know, it seems to be kind of never ending. We never lost any client funds but its getting to the point where it could happen.

Cavirtex joins a long list of Bitcoin exchanges to experience the attention of virtual currency hackers:

In May 2012 Bitcoinica was allegedly fleeced out of $225,000 before experiencing a further $90,000 loss later that same year.

September 2012 saw the then fourth largest exchange Bitfloor lose $250,000 after an encryption lapse during a server upgrade.

Various small exchanges in Australia, China and Denmark disappeared in November 2013, along with investors' cash, after claiming they'd been hacked.

2014 saw the fall of the greatest exchange, as Mt. Gox announced it had lost around half-a-billion dollars worth of Bitcoins following alleged insider fraud.

More recently, Bitstamp suspended its service after losing $5 million in

BTC after hackers targeted its hot wallet and then, earlier this week, Chinese exchange Bter claimed to have lost $1.75 million after its cold wallet system was hacked.

For all its attractiveness as an alternative currency, Bitcoin and the associated trading of the currency still appears to be a bit wet behind the ears - so it may be wise to think twice before putting all your virtual coins in one virtual basket.

=~=~=~=